(19) 世界知的所有権機関 国際事務局



(43) 国際公開日 2001年9月13日(13.09.2001)

PCT

(10) 国際公開番号 WO 01/67605 A1

青葉区一番町1丁目2番25号 富士通東北ディジタル・

テクノロジ株式会社内 Miyagi (JP). 山下直人 (YA-

MASHITA, Naoto) [JP/JP]. 宮本宗易 (MIYAMOTO,

Muneyasu) [JP/JP]; 〒211-8588 神奈川県川崎市中原 区上小田中4丁目1番1号富士通株式会社内 Kanagawa

(51) 国際特許分類": H03K 3/84, H04J 13/00, H04L 9/20

(21) 国際出願番号:

PCT/JP00/01427

(22) 国際出願日:

2000年3月9日(09.03.2000)

(25) 国際出願の言語:

日本語

(74) 代理人: 伊東忠彦(ITOH, Tadahiko); 〒150-6032 東京 都渋谷区恵比寿4丁目20番3号 恵比寿ガーデンプレ

(26) 国際公開の言語:

日本語

イスタワー32階 Tokyo (JP).

(71) 出願人 (米国を除く全ての指定国について): 富士通 株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神 奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP).

(81) 指定国 (国内): JP, US.

添付公開書類:

(JP).

国際調査報告書

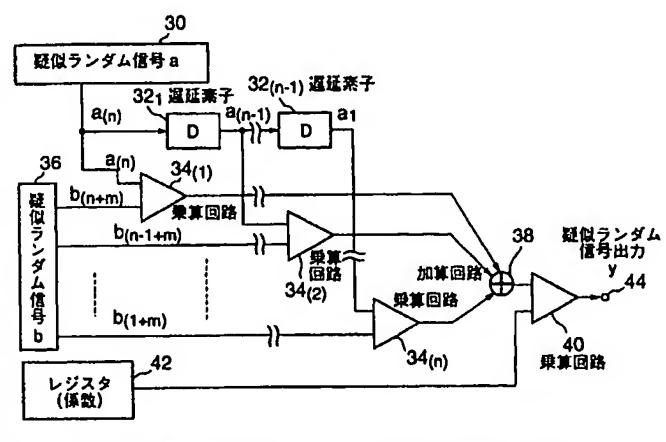
(72) 発明者; および

(SUZUKI, Toshiya) [JP/JP]; 〒980-0811 宮城県仙台市 のガイダンスノート」を参照。

2文字コード及び他の略語については、 定期発行される (75) 発明者/出願人 (米国についてのみ): 鈴木俊哉 各PCTガゼットの巻頭に掲載されている「コードと略語

(54) Title: METHOD AND APPARATUS FOR PRODUCING PSEUDORANDOM SIGNAL

(54) 発明の名称: 疑似ランダム信号生成方法及びその装置



(57) Abstract: A cross-correlation function is derived from two pseudorandom signals of small cross-correlation, and the value of the cross-correlation function is used as a new pseudorandom signal. Since the phase and amplitude of the new pseudorandom signal are random, a number of new pseudorandom signals can be generated from any two of a plurality of existing pseudorandom signals.

30...PSEUDORANDOM SIGNAL a

36...PSEUDORANDOM SIGNAL b

32 (n-1) ... DELAY ELEMENT

38...ADDER

32(1)...DELAY ELEMENT

40...MULTIPLIER

34(2)...MULTIPLIER

42...REGISTER (COEFFICIENT)

34(n)...MULTIPLIER

34(1)...MULTIPLIER

44...PSEUDORANDOM SIGNAL OUTPUT y

•}

(57) 要約:

本発明は、互いに相関の小さな2つの疑似ランダム信号を用い、前記2つの疑似ランダム信号の相互相関関数を生成し、前記相互相関関数の値を新たな疑似ランダム信号として出力するように構成することで、新たな疑似ランダム信号はそれ自体、位相も振幅もランダムとなり、既存の疑似ランダム信号が複数あれば、そのうちの2つを選択して多数の新たな疑似ランダム信号を生成することができる。

明細書

疑似ランダム信号生成方法及びその装置

5 技術分野

本発明は、疑似ランダム信号生成方法及びその装置に関し、特に、鍵としての暗号やCDMA方式の拡散符号等に用いられる疑似ランダム信号を生成する疑似ランダム信号生成方法及びその装置に関する。

10 背景技術

従来から鍵としての暗号やCDMA(符号分割多元接続)方式の拡散信号として疑似ランダム信号が用いられている。従来の疑似ランダム信号の作成方法としては次に示すようなものがある。

第1の方法は、各種の疑似ランダム系列(2値信号列)を作成して使用する方法である。従来から疑似ランダム系列にはいくつか種類があり、M(最大周期系列)系列、ゴールド系列、バーカー系列およびM系列から派生した各種の系列がある。これらの信号振幅は2値(0と1)で、位相がランダムである。これらの系列(2値信号列)を適当な値にレベル変換して、信号として用いると疑似ランダム信号となる。

20 これらの疑似ランダム信号は、生成元である生成多項式が違えば位相が異なるので、違った別の信号となる。また、異なる系列同士の相互相関は、その系列自身の自己相関とは違った性質を示し、この性質を使って2つの信号が同じものか、異なるものかを区別することができる。また、生成多項式から作られるので、ランダムとはいっても周期信号になる。ただし、1周期内ではランダムな信号になる。これらの性質から、CDMA方式に使用する拡散信号に適している。

第2の方法は、自然界のノイズを使用する。自然界には、熱雑音などランダム信号として使用できそうな信号が存在する。これには数多くの種類があるが、いずれもランダムで再現性がない。これらの理由から、CDMA方式に使用する拡散信号にはあまり用いられない。また、システム同定用の信号としては、正規性

ならびにスペクトルの性質が許容できる範囲のものを選定し、これに用いられている。

従来の第1の方法により生成される疑似ランダム信号は、その数が制限される。 疑似ランダム信号の個数は、その種類ごとに理論的に決まっている。CDMA通 信方式の場合、拡散信号として使用する疑似ランダム信号の個数がそのままチャ ネル数となるので、疑似ランダム信号の個数に制限があるとチャネル数を増加さ せることに限界があるという問題があった。

また、近年インターネットでの商取引が注目されはじめてから、インターネット商取引の鍵としての暗号が注目されており、さらに安全性を高めることが必要とされている。この安全性を高めるために、暗号自体の複雑さを増加させると同時に、暗号自体の数を増加させることが重要となる。一般的に暗号解読の困難さは、任意の時間的計算手法、つまりコンピュータを使って鍵としての暗号を見つけ出そうとする方法を用いた場合、その鍵としての暗号にたどり着く確率として定義されている。この確率が小さいさければ小さいほど、解読困難な暗号となる。つまり、暗号自体の数が多ければ、その暗号にたどり着く時間が増し解読は困難になるからである。しかるに、従来の第1の方法により生成される疑似ランダム信号は、その数が制限されるため、暗号の安全性を高めるのに限界があるという問題があった。

20 発明の開示

本発明は、既存の疑似ランダム信号を用いて新たな疑似ランダム信号を生成でき、疑似ランダム信号数を増加することができる疑似ランダム信号生成方法及びその装置の提供を総括的な目的とする。

この目的を達成するため、本発明は、互いに相関の小さな2つの疑似ランダム信号を用い、前記2つの疑似ランダム信号の相互相関関数を生成し、前記相互相関関数の値を新たな疑似ランダム信号として出力するように構成される。

このような疑似ランダム信号生成方法によれば、既存の2つの疑似ランダム信号の相互相関関数を生成して新たな疑似ランダム信号を生成するため、新たな疑似ランダム信号はそれ自体、位相も振幅もランダムとなり、既存の疑似ランダム

信号が複数あれば、そのうちの2つを選択して多数の新たな疑似ランダム信号を 生成することができる。

図面の簡単な説明

5 本発明の他の目的、特徴及び利点は添付の図面を参照しながら以下の詳細な説明を読むことにより一層明瞭となるであろう。

図1は、本発明の疑似ランダム信号生成装置の第1実施例のブロック図である。

図2は、本発明の疑似ランダム信号生成装置の第2実施例のブロック図である。

図3は、本発明の疑似ランダム信号生成方法の様子を示す図である。

10 図4は、M系列疑似ランダム信号の各データの値、最小値、平均値、最大値、 標準偏差を示す図である。

図5は、本発明で生成した新たな疑似ランダム信号の各データの値、最小値、 平均値、最大値、標準偏差を示す図である。

図6(A)は、同一のランダム信号の自己相関関数を示す図である。

15 図 6 (B) は、異なるランダム信号の自己相関関数を示す図である。

図7は、M系列疑似ランダム信号から得られる自己相関関数を示す図である。

図8は、M系列疑似ランダム信号から得られる相互相関関数を示す図である。

図9は、本発明方法で生成した新たな疑似ランダム信号から得られる自己相関 関数を示す図である。

20 図10は、本発明方法で生成した新たな疑似ランダム信号から得られる相互相 関関数を示す図である。

発明を実施するための最良の形態

以下、本発明の実施例を図面に基づいて説明する。

25 本発明では、互いに相関の小さい、または相関のない2つの擬似ランダム信号を用い、2つの擬似ランダム信号の相互相関関数を計算し、相互相関関数から1つの擬似ランダム信号を得る。

擬似ランダム信号が離散周期信号つまりディジタル周期信号の場合、(1)式により、2つの擬似ランダム信号 a [=a(1), ..., a(n)], b [=b]

(1), …, b (n)] から新たな擬似ランダム信号 y [=y(1), …, y (m)] を生成する。だだし、n, mは $1\sim$ Nの整数であり、Nは擬似ランダム信号のデータ数 (即ち周期であり、擬似ランダム信号が2値信号列の場合はビッ

5

15

30

$$y (m) = \frac{1}{N} \sum_{n=0}^{N} a (m) \cdot b (n+m) \cdots (1)$$

ト数) である。一例ではN=31である。

10 新たな擬似ランダム信号yをソフトウエアで生成する場合は、基本的に、この (1) 式をそのまま利用する。また、新たな擬似ランダム信号yをディジタル回 路で生成する場合は図1に示す装置を用いる。

図1は、本発明の疑似ランダム信号生成装置の第1実施例のブロック図を示す。この実施例はフーリエ変換での畳み込み計算を行うものである。同図中、レジスタ10には例えばNデータの疑似ランダム信号 a が格納されており、レジスタ10からパラレルに出力される疑似ランダム信号 a は高速フーリエ変換器(FFT)12でフーリエ変換され、ここで得られた複素数のフーリエ変換値は符号反転回路14にて虚部の符号を反転されて乗算回路16に供給される。

また、レジスタ18にはNデータの疑似ランダム信号bが格納されており、レジスタ18から出力される疑似ランダム信号bは乗算回路16に供給され、虚部の符号を反転された複素数のフーリエ変換値と乗算される。これにより得られた複素数の値は逆フーリエ変換器20に供給される。逆フーリエ変換器20は上記複素数の値の逆フーリエ変換を行い、(1)式で表される新たな疑似ランダム信号yを生成して出力する。この新たな疑似ランダム信号yは乗算回路22において、レジスタ24から供給されるデータ数Nを乗算されて端子26から出力される。

なお、(1)式で表される新たな疑似ランダム信号y [=y(1), …, y (m)]の各データは相互相関関数の値そのもの、つまり実数値であるため、これを使用するのに便利な整数値とするために、乗算回路22でデータ数Nを乗算したのち出力している。また、実数で使用する場合は、Nの代わりに目的にあっ

た係数を乗算する。

10

図 2 は、本発明の疑似ランダム信号生成装置の第 2 実施例のブロック図を示す。この実施例は(1)式をそのまま計算するものである。同図中、レジスタ 3 0 には例えばNデータの疑似ランダム信号 a が格納されており、レジスタ 3 0 から単位時間毎に疑似ランダム信号 a のデータ a (1), a (2), …, a (n)が順次読み出されて遅延素子 3 2 (1)に供給され、縦続接続された遅延素子 3 2 (1), 3 2 (2), …, 3 2 (n-1)で遅延される。遅延素子 3 2 (1)~3 2 (n-1) それぞれは単位時間の遅延を行う。レジスタ 3 0 から読み出されたデータ及び遅延素子 3 2 (1)~3 2 (n-1) それぞれの出力データは乗算回路 3 4 (1)~3 4 (n)に供給される。

また、シフトレジスタ36には例えばNデータの疑似ランダム信号bが格納されており、シフトレジスタ36から同時に読み出される疑似ランダム信号bのデータb (1+m) ~b (n+m) は乗算回路34 (n) ~34 (1) に供給され、レジスタ30からデータa (n) が読み出されたタイミングで疑似ランダム信号aのデータa (1) ~a (n) それぞれと乗算される。乗算回路34 (n) ~34 (1) それぞれの出力は、加算回路38で加算されて新たな疑似ランダム信号 (n) ぞれぞれの出力は、加算回路38で加算されて新たな疑似ランダム信号 (n) でデータ (n) が得られる。このデータ (n) は乗算回路40において、レジスタ42から供給される目的にあった係数を乗算されて、端子26から出力される。

20 この装置では、シフトレジスタ36でNデータの疑似ランダム信号 b を出力する位置を順次シフトすることにより、mを1から順にNまで変化させて逐一データy (m)を計算する。このため、図1の実施例に比べて計算回数及び時間が大となるが、レジスタと遅延素子と乗算回路と加算回路で構成されるために、回路構成が簡単になる。このため、疑似ランダム信号のデータ数Nが小さい場合は図25 2の回路を使用し、疑似ランダム信号のデータ数Nが大きい場合は図1の回路を使用するというように使い分けても良い。

本発明では、互いに相関の小さい2つの擬似ランダム信号を用い、2つの擬似ランダム信号の相互相関関数を計算し、相互相関関数から1つの擬似ランダム信号を得る。このため、A個の擬似ランダム信号から2個の擬似ランダム信号を選

んで生成できる新たな擬似ランダム信号の個数Bは(2)式で表される。

B = A! / [2 (A-2)!] ... (2)

10

15

例えばA=100の場合にはB=4950となる。さらに、(1)式で生成された新たな疑似ランダム信号と元の疑似ランダム信号の相互相関関数、または新たな疑似ランダム信号同士の相互相関関数もまた、疑似ランダム信号として使える。図3に本発明の疑似ランダム信号生成方法の様子を示す。

図3において、まず疑似ランダム信号1,2を用意し、それを用いて新たな疑似ランダム信号3を作る。同じ手法で、疑似ランダム信号1と疑似ランダム信号3から疑似ランダム信号4が、また疑似ランダム信号2と疑似ランダム信号3から疑似ランダム信号5を作ることができる。この方法を繰り返すことで、疑似ランダム信号6,7,8等、多くの疑似ランダム信号を作ることができる。これらの新たな疑似ランダム信号はそれ自体、位相も振幅もランダムな信号であるので、同じ疑似ランダム信号が複数できるおそれはほとんどない。このことから、疑似ランダム信号が最初にA個あったとすると、その中の任意の2つを選ぶことでB個の疑似ランダム信号を作ることができる。さらに、そのB個の疑似ランダム信号を作ることができる。さらに多くの疑似ランダム信号を作ることができ、その数に制限は無い。

図4に、データ数が31の6個のM系列疑似ランダム信号(2,5)、(2,3,4,5)、(1,2,4,5)、(3,5)、(1,2,3,5)、(1,2)、(1,2,3,5)、(1,2) (1,2

図5に、上記のM系列疑似ランダム信号から生成した新たな疑似ランダム信号を示す。左端の列から順にM系列疑似ランダム信号(2,5)と(2,3,4,25)から生成した新たな疑似ランダム信号(25-2345)、M系列疑似ランダム信号(2,5)と(1,2,4,5)から生成した新たな疑似ランダム信号(25-1245)、M系列疑似ランダム信号(2,5)と(3,5)から生成した新たな疑似ランダム信号(2,5)と(1,2,3,5)から生成した新たな疑似ランダム信号(2,5)と(1,2,3,5)から生成した新たな疑似ランダム信号(25-123

5)、M系列疑似ランダム信号(2,5)と(1,3,4,5)から生成した新たな疑似ランダム信号(25-1345)を示す。

更に、疑似ランダム信号(25-2345)と(2,5)から生成した新たな 疑似ランダム信号(25-2345)-(25)、疑似ランダム信号(25-1 245)と(2,5)から生成した新たな疑似ランダム信号(25-1245) -(25)、疑似ランダム信号(25-35)と(2,5)から生成した新たな 疑似ランダム信号(25-35)-(25)、疑似ランダム信号(25-123 5)と(2,5)から生成した新たな疑似ランダム信号(25-1235)-(25)、疑似ランダム信号(25-1345)と(2,5)から生成した新た な疑似ランダム信号(25-1345)と(2,5)から生成した新た な疑似ランダム信号(25-1345)-(25)を示す。図5でも図4と同様 に各データの値の他に最小値、平均値、最大値、標準偏差をあわせて示す。これ らの新たな疑似ランダム信号は各データが多値の多値系列である。

本実施例で生成した疑似ランダム信号と他の疑似ランダム信号(例えばM系列 疑似ランダム信号)とは、両者の自己相関関数を計算することで区別できる。す なわち、もし両者が同一のランダム信号であれば、自己相関関数は図6(A)に 示すように1周期の最初でデルタ関数のように高い値となり、それ以外の場所で は非常に小さな値になる。また、両者が異なる疑似ランダム信号であれば、図6 (B) に示すように1周期の全般に渡って任意の値となる自己相関関数が得られ る。

15

20 図7は、図4に示すM系列疑似ランダム信号(2,5)と、M系列疑似ランダム信号(2,5)とから得られる相互相関関数、つまり自己相関関数を示す。図8は、図4に示すM系列疑似ランダム信号(2,5)と、M系列疑似ランダム信号(2,3)とから得られる相互相関関数を示す。また、図9は、本発明方法で生成した図5に示す新たな疑似ランダム信号(25-2345)と、本発明方法で生成した新たな疑似ランダム信号(25-2345)とから得られる相互相関関数、つまり自己相関関数を示す。図10は、本発明方法で生成した図5に示す新たな疑似ランダム信号(25-2345)と、本発明方法で生成した図5に示す新たな疑似ランダム信号(25-2345)と、本発明方法で生成した新たな疑似ランダム信号(25-1245)とから得られる相互相関関数を示す。

また、CDMA通信方式において、本発明によって生成された擬似ランダム信号を拡散信号として用いることにより、CDMA通信のチャネル数を更に増やすことができる。疑似ランダム信号の組み合せは任意につくれるので、現状の方法よりも数多くの拡散信号が作れる。また、この手法を繰り返すことによってさらに多くの拡散信号が作れるので、チャネルの大幅な増加を期待できる。原理的にはチャネル数に制限はない。

本発明により生成された疑似ランダム信号は、インターネット上の電子商取り引きに必要な鍵としての暗号として使うことができる。電子商取り引きの鍵としての暗号としては、第1に暗号を使用するものにとっては作成しやすい。第2に暗号を解読しようとする敵に取っては解読が難しい、といった性質が必要である。このような関係を一方向関数という。本発明により生成された疑似ランダム信号は、信号自体ランダムであり、かつその数を非常に多く増やせる。つまり、敵にとっては多数の中から、鍵としての暗号に適合した信号を見つけなければならず、なおかつランダムな性質のため、解読がたいへん困難になる。この暗号を作成する側にとっては、容易に作成することができる。

10

15

20

25

更に、本発明により生成された疑似ランダム信号は、システム同定のためのインパルス信号として使用することができる。一般的なシステム同定方法としては、あるシステムにインパルス信号を入力してインパルス応答を求める方法が用いられる。しかし、インパルス信号は作成が難しいなどの問題があるため、通常はホワイトノイズの特性に類似した性質を持つ疑似ランダム信号が用いられるこの疑似ランダム信号には、統計学上の扱いやすさから正規性(ランダム変数として正規分布を有すること)が求められる。従来のM系列疑似ランダム信号等は低域フィルタを通したときに正規性を有し、また、低域フィルタのカットオフ周波数が疑似ランダム信号の種類により異なる所定範囲からはずれた場合には正規性からはずれた信号となる。このため、従来のM系列疑似ランダム信号等をインパルス信号として使用することは困難であった。しかし、本発明で生成された疑似ランダム信号は周波数スペクトルが、その信号自身の持つ最高周波数までフラットで広い周波数帯域にわたって正規性を有し、ホワイトノイズに類似した性質をもつ。このようにホワイトノイズに類似した性質を持っているので、低域フィルタを通

す必要がなく、上記のシステム同定に用いることができる。

請求の範囲

1. 2つの疑似ランダム信号を用い、前記2つの疑似ランダム信号の相互相関 関数を生成し、前記相互相関関数の値を新たな疑似ランダム信号として出力する 疑似ランダム信号生成方法。

2. 2つの疑似ランダム信号を用い、前記2つの疑似ランダム信号の相互相関 関数を生成し、前記相互相関関数の値を新たな疑似ランダム信号として出力する 疑似ランダム信号生成装置。

10

3. 請求項2記載の疑似ランダム信号生成装置において、

第1の疑似ランダム信号のフーリエ変換を行うフーリエ変換器と、

前記フーリエ変換器の出力値の虚部の符号を反転する符号反転回路と、

前記符号反転回路の出力値と第2の疑似ランダム信号との乗算を行う第1の乗 15 算回路と、

前記第1の乗算回路の出力値の逆フーリエ変換を行って前記新たな疑似ランダム信号として出力する逆フーリエ変換器とを

有する疑似ランダム信号生成装置。

20 4. 請求項3記載の疑似ランダム信号生成装置において、

前記逆フーリエ変換器の出力値に所定の係数を乗算する第2の乗算回路を有する疑似ランダム信号生成装置。

- 5. 請求項2記載の疑似ランダム信号生成装置において、
- 25 第1の疑似ランダム信号を構成する各データと第2の疑似ランダム信号を構成 する各データとの乗算を行う複数の第3の乗算回路と、

前記複数の第3の乗算回路の出力値を加算して前記新たな疑似ランダム信号を 構成するデータとして出力する加算器と、

第2の疑似ランダム信号を構成する各データをシフトして前記複数の第3の乗

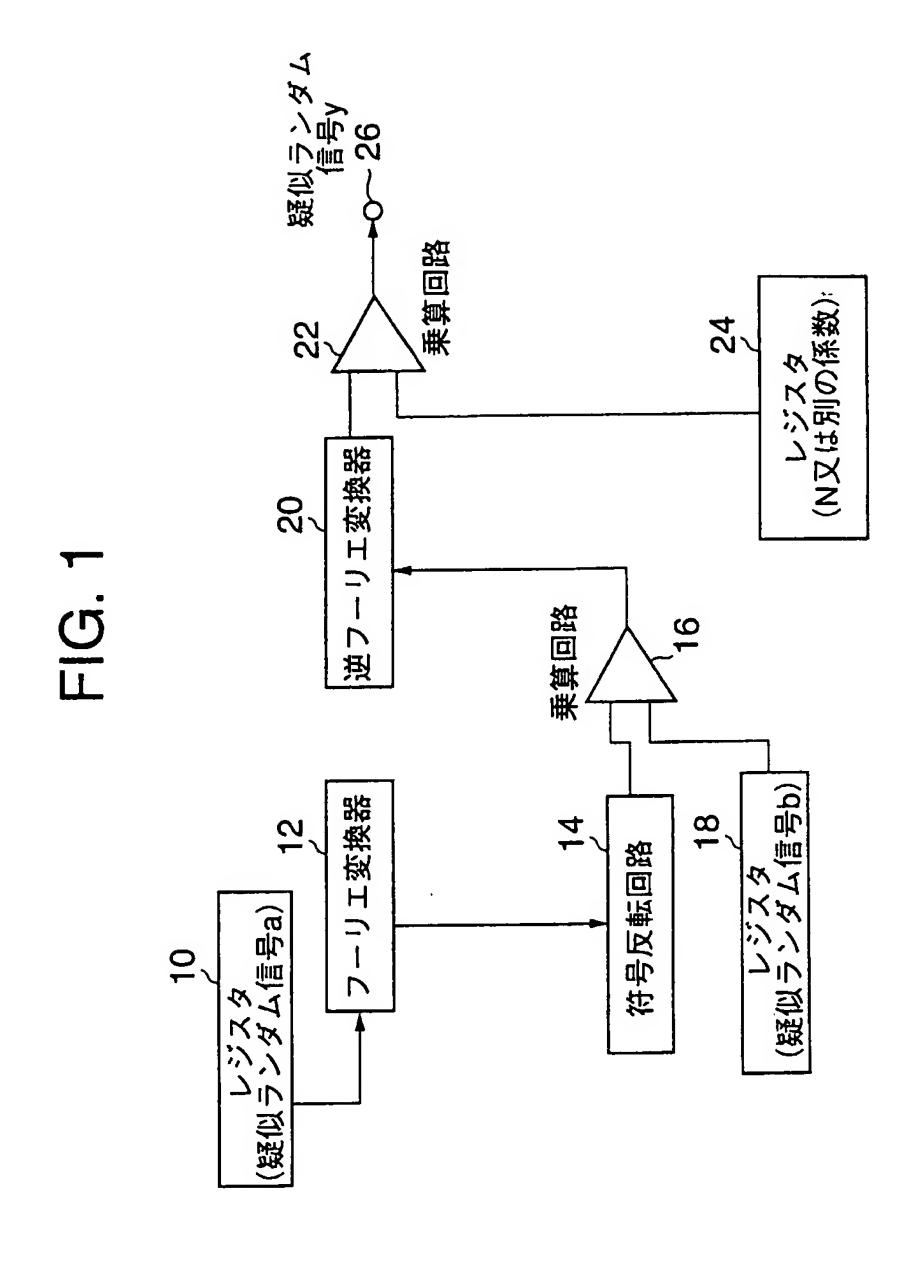
算回路に供給して前記新たな疑似ランダム信号を構成する各データを得るシフト レジスタとを

有する疑似ランダム信号生成装置。

15

- 5 6. 請求項5記載の疑似ランダム信号生成装置において、
 - 前記加算器の出力値に所定の係数を乗算する第4の乗算回路を有する疑似ランダム信号生成装置。
 - 7. 請求項2記載の疑似ランダム信号生成装置において、
- 10 前記新たな疑似ランダム信号をCDMA方式の拡散信号として使用する疑似ランダム信号生成装置。
 - 8. 請求項2記載の疑似ランダム信号生成装置において、 前記新たな疑似ランダム信号を鍵としての暗号として使用する疑似ランダム信 号生成装置。
 - 9. 請求項2記載の疑似ランダム信号生成装置において、

前記新たな疑似ランダム信号をシステム同定のためのインパルス信号として使 用する疑似ランダム信号生成装置。



疑似ランダム 信号出力 40 乗算回路 38 加算回路 乗算回路 34(n) 32(n-1) 遅延素子 al -| | (2) | (3) | (3) | (4) | (5) | (5) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | (6) | 乗算回路 321 遅延素子 34(1) 30 b(n-1+m) 疑似ランダム信号a 42 b(1+m) a(n) p(n+m) a(n) アジスタ(密数) 36 疑似ランダム信号 b

FIG. 3

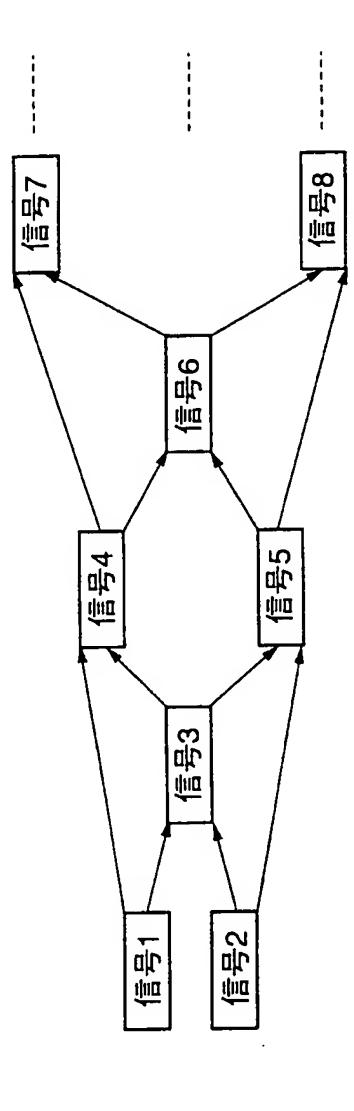


FIG. 4

系列 (1,3,4,5)	-	-		-				-	-1	+ -	•	T-	-	-			•	T-		-	-	7	-	•	Ţ-	-	V	•	1	-	-	-1.0	0.0	1.0	1.017095255
·列(1,2,3,5) M系列	T	1	-1	-1	-1	1-	•	1	-1	-1	-	-1	-	-	,	-	1	-	Τ-	~	—	-	Τ-	T -	-1	-	-	•	7-	-	-	-1.0	0.0	1.0	.017095255
M系列 (3,5) M系列	-	-1	-1	1	1	-	•	1-	•	1-	•	1	-1	1	1	1	-1	•		T	-1	-1	-1	-1		-	T	•	-	•	-	-1.0	0.0	1.0	1.017095226 1
M系列 (1,2,4,5)		-	•	 -	•	-	•	 -	—		-	-1	-1	-1	 -	1	1	1-	1	1-		1-	1-	1	 -		•		-	Y	-	-1.0	0.0	1.0	1.017095255
M系列 (2,3,4,5)	-	_	-	•	-1-	-	-		-	-	-	•		ļ		-	-	 -	-	1-			~	-	1-	1-	-1	•	-		1	-1.0	0.0	1.0	1.017095255
M系列 (2,5)		-	-	-	•	-	-		-	-	-		-	-	T-	T	1	-	•	•		1	•	-	-		J -	•	1-			-1.0	0.0	1.0	1.017095255
E						9		8			7		13			16													29			M	AVE	MAX	

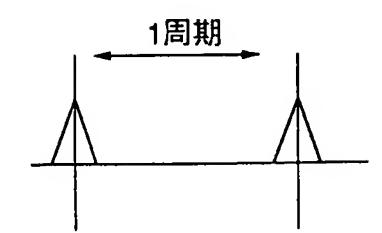
PCT/JP00/01427

FIG. 5

ランダム(25-1345)-(25)	31.0	0.1-	31.0	0.1.	0.1-	31.0	1.0	01.	01	[0]	-65.0	1.0	31.0	10	-65.0	-65.0	31.0	10	31.0	310	1.0	10	10	-650	310	920	310	310	10	10	310	-65.0	00	310	32.5120323
	31.0	0.1.	31.0	31.0	31.0	1.0]	0.1.	31.0]	-1.0]	1.0	31.0	-1.0	-1.0	0'1-	-1.0	65.0	31.0	-65.0]	-1.0	31.0	-1.0	31.0	100	1.0	-1.0	-65.0	-65.0	31.0	31.0	0.1.	-65.0	0.59	000	31.0	32.5120326
ランダム(25-35)-(25)	31.0	23.0	7.0	0.64-	0.7	23.0	23.0	10.71-	23.0	-49.0	23.0	17.0	-49.0	17.0	17.0	0.68-	31.0	31.0	23.0	31.0	7.0	23.0	-49.0	31.0	70	7.0	230	23.0	23.0	-49.0	-17.0	-89.0	0.0	31.0	32.51203249
ランダム(25-1245)-(25)	-17.0	-17.0	15.0	0'6	15.0	0'1-	01.	31.0	49.0	-17.0	1.0	-17.0	15.0]	15.0	1.0	-49.0	0,1.0	15.0	1.0	-1.0	-101		111.0	31.0	31.0	-49.0	31.0	.17.0	-49.0	-1.0	31.0		0.0	(110	32,51203294
ランダム(25-2345)-(25)	-1.0	-17.0	0:83	0.1-	63.0	83.0 83.0	0.64-	.33.0	.33.0	17.0	33.0	15.0	0.71-	1.0	-33.0	15.0	15.0	0.71-	10.71-	10.71-	1011-	0.0	-33.0	0.71	15.01	0'1-	15.0	-17.0	10.71.	[0:33	0'21:	0'6	0.0	0°C9	
ランダム25-1345	-1.0]	•1.0	0'.2	0.1.	-1.0	7.0	0.1-	7.0	-1.0	0.6-	10.7	1.0	0.1-	1.0	1.0	0.7	7.0	0.6-	-1.0	1.0	0.7	-9.0	1.0	0.6	0.6-	0.6-	0.7	0.7	0.1-	7.0	-1.0	0.6-	0.0		5.747369
ランダム25-1235	7.0	0.6-	0.1.	-1.0	-1.0	7.0	-1.0	7.0	-1.0	0.6-	0.7	-1.0	0.7	-1.0	-1.0	0.1.	-1.0	7.0	7.0	-1.0	-1.0	7.0	-1.0	-1.0	0.6-	0.6-	0.6-	7.0	0.6-	-1.0	7.0	-9.0	0.0	7.0	5.747369674
ランダム25-35	7.0	0.6-	7.0	7.0	11.0	-1.0	-1.0	3.0	-1.0	-5.0	3.0	0.6-	1.0	-5.0	-5.0	3.0	3.0	3.0	0.6-	7.0	1.0	3.0	-5.0	0.6-	-5.0	3.0	3.0	7.0	3.0	0.6-	3.0	-9.0	0.0	11.0	5.747369663
ランダム25-1245	7.0	7.0	10.7	1.0	0.00	1.0	7.0	1.0	-1.0 -1.0	0.1-	0.1-	0.6-	1.0	0:	0.6-	0:1:0	7.01	0.6-	1.0	0,1-	7.0	7.0	7.0	0.6-	7.0	-1.0	0.1.	0.1-	0.6-	7.0	1.0	0.6-	0.0	7.0	5,74736741
ランダム25-2345 ラ	7.0	7.0	0.1-	1.0	7.0	7.0	0.6-	7.0	0.6-	1.0	0.1.	0.1.	7.0	7.0	0.1	10'2	0.6-	0.6-	0.1.	7.0	0.1.	0.6-	-1.0	0.1	-1.0	-1.0	0.6.	-10	1.0	10.7	-1.0	0.6-	0.0	7.0	5.747369711
E	-	2	3	4	5	9	7	8	O	10	=	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	53	30	31	NIW	AVE	MAX	Û

FIG. 6(A)

FIG. 6(B)



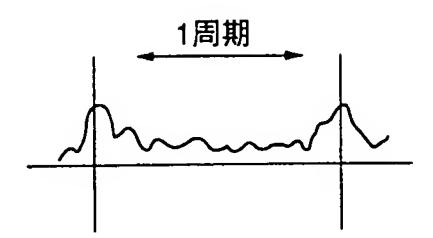


FIG. 7

	信号データA	信号データA	相互相関関数
1	1	1	1.000
2	-1	-1	-0.032
3	1	1	-0.032
4	1	1	-0.032
5	-1	-1	-0.032
6	-1	-1	-0.032
7	-1	-1	-0.032
8	1	1	-0.032
9	1	1	-0.032
10	1	1	-0.032
11	1	1	-0.032
12	1	1	-0.032
13	-1	-1	-0.032
14	-1	-1	-0.032
15	1	1	-0.032
16	1	1	-0.032
17	-1	-1	-0.032
18	1	1	-0.032
19	-1	-1	-0.032
20	-1	-1	-0.032
21	1	1	-0.032
22	-1	-1	-0.032
22 23	-1	-1	-0.032
24	-1	-1	-0.032
25	-1	-1	-0.032
26	1	1	-0.032
27	-1	1	-0.032
28	1	1	-0.032
29	-1	-1	-0.032
30	1	1	-0.032
31	1	1	-0.032
MIN	-1.0	-1.0	
AVE	0.0	T	
MAX	1.0		
σ	1.01709526		

FIG. 8

	信号データA	信号データB	相互相関関数
1	1	-1	0.226
2	-1	1	0.226
3	1	-1	-0.032
4	1	1	-0.032
5	-1	-1	0.226
6	-1	-1	0.226
7	-1	-1	-0.290
8	1	1	0.226
9	1	1	-0.290
10	1	1	-0.032
11	1	-1	-0.032
12	1	1	-0.032
13	-1	1	0.226
14	-1	1	0.226
15	1	1	-0.032
16	1	1	0.226
17	-1	-1	-0.290
18	1	-1	-0.290
19	-1	1	-0.032
20	-1	-1	0.226
21	1	-1	-0.032
22	-1	1	-0.290
23	-1	1	-0.032
24	-1	1	-0.032
25	-1	-1	-0.032
26	1	-1	-0.032
27	-1	-1	-0.290
28	1	1	-0.032
29	-1	-1	-0.032
30	1	1	0.226
31	1	1	-0.032
MIN	-1.0	-1.0	
AVE	0.0	Y	
MAX	1.0	1	
σ	1.01709526		

FIG. 9

	信号データC	信号データC	相互相関関数
1	7.0	7.0	31.968
2	7.0	7.0	-1.065
3	-1.0	-1.0	-1.065
4	-1.0	-1.0	-1.065
5	7.0	7.0	-1.065
6	7.0	7.0	-1.065
7	-9.0	-9.0	-1.065
8	7.0	7.0	-1.065
9	-9.0	-9.0	-1.065
10	-1.0	-1.0	-1.065
11	-1.0	-1.0	-1.065
12	-1.0		-1.065
13	7.0		-1.065
14	7.0		-1.065
15	-1.0		-1.065
16	7.0		-10.65
17	-9.0		-1.065
18	-9.0		-1.065
19	-1.0		-1.065
20	7.0		-1.065
21	-1.0		-1.065
22	-9.0		-1.065
23	-1.0		-1.065
24	-1.0	-1.0	-1.065
25	-1.0	-1.0	-1.065
26	-1.0	-1.0	-1.065
27	-9.0	-9.0	-1.065
28	-1.0	-1.0	-1.065
29	-1.0		-1.065
30	7.0		-1,065
31	-1.0		-1.065
MIN	-9.0	-9.0	
AVE	0.1	0,1	
MAX	7.0		
σ	5.84237399	5.842374	

FIG. 10

	信号データC	信号データD	相互相関関数
1	7.0	7.0	-1.065
2	7.0		7.194
3	-1.0		7.194
4	-1.0		-1.065
5	7.0		-9.323
6	7.0		-1.065
7	-9.0	7.0	-1.065
8	7.0	-1.0	-1.065
9	-9.0	-1.0	-1.065
10	-1.0	-1.0	7.194
11	-1.0	-1.0	-9.323
12	-1.0		-1.065
13	7.0		-1.065
14	7.0	-1.0	-9.323
15	-1.0	-9.0	-1.065
16	7.0	-1.0	-1.065
17	-9.0		-9.323
18	-9.0		7.194
19	-1.0		7.194
20	7.0	-1.0	7.194
21	-1.0	7.0	7.194
22	-9.0	7.0	-1.065
23	-1.0	7.0	7.194
24	-1.0	-9.0	-9.323
25	-1.0	7.0	7.194
26	-1.0	-1.0	-1.065
27	-9.0	-1.0	-1.065
28	-1.0	-1.0	-1.065
29	-1.0		7.194
30	7.0		-1.065
31	-1.0	-1.0	-9.323
MIN	-9.0		
AVE	0.1	0.1	
MAX	7.0	7.0	
σ	5.84237399		

INTERNATIONAL SEARCH REPORT

(p t₁ - 5 - 6

International application No.

PCT/JP00/01427

	IFICATION OF SUBJECT MATTER C1 H03K 3/84, H04J 13/00, H0	4L 9/20,	
According to	International Patent Classification (IPC) or to both nat	ional classification and IPC	
	SEARCHED		
Int.	ocumentation searched (classification system followed back 3/84, H04J 13/00, H0	4L 9/20, G06F 7/58,	
Jits Koka	ion searched other than minimum documentation to the uyo Shinan Koho 1926-1996 i Jitsuyo Shinan Koho 1971-1996		
	ata base consulted during the international search (name	e of data base and, where practicable, sear	rch terms used)
C. DOCU	MENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where app	propriate, of the relevant passages	Relevant to claim No.
A	JP, 57-41028, A (Yasushi ISHII) 06 March, 1982 (06.03.82), Figs. 1, 4, 7, 8 and their expl (Family: none)		1 - 9
A	JP, 63-2419, A (Fujitsu Limited 07 January, 1988 (07.01.88), Figs. 1, 2 and their explanation (Family: none)		1 - 9
A	JP, 3-181238, A (TOKIMEC INC.), 07 August, 1991 (07.08.91) (Fa		1 - 9
A	JP, 4-5773, A (TOKIMEC INC.), 09 January, 1992 (09.01.92) (Family: none)	1 - 9
- Eureba	- documents are listed in the continuation of Box C	See patent family annex.	
* Special docume consider date docume cited to special docume means "P" docume than the	categories of cited documents: ent defining the general state of the art which is not ered to be of particular relevance document but published on or after the international filing ent which may throw doubts on priority claim(s) or which is establish the publication date of another citation or other reason (as specified) ent referring to an oral disclosure, use, exhibition or other ent published prior to the international filing date but later e priority date claimed	"T" later document published after the interpriority date and not in conflict with the understand the principle or theory understand to enside the considered novel or cannot be considered to step when the document is taken alone document of particular relevance; the considered to involve an inventive step combined with one or more other such combination being obvious to a person document member of the same patent in the principle." Date of mailing of the international sear	ne application but cited to erlying the invention cannot be red to involve an inventive claimed invention cannot be claimed invention cannot be when the document is a documents, such a skilled in the art family
06 3	actual completion of the international search June, 2000 (06.06.00)	27 June, 2000 (27.06	
	nailing address of the ISA/ anese Patent Office	Authorized officer	
Facsimile N		Telephone No.	

A. 発明の風する分野の分類(国際特許分類(IPC))		
Int. Cl' H03K 3/84, H04J 13/00,	H04L 9/20,	
B. 調査を行った分野 調査を行った最小限資料(国際特許分類(IPC))		
Int. Cl' H03K 3/84, H04J 13/00,	H04L 9/20, G06F 7/58,	
最小限資料以外の資料で調査を行った分野に含まれるもの		
日本国実用新案公報 1926 - 1996 日本国公開実用新案公報 1971 - 1996		
国際調査で使用した電子データベース(データベースの名称、	調査に使用した用語)	
C. 関連すると認められる文献		
引用文献の カテゴリー* 引用文献名 及び一部の箇所が関連する	ときは、その関連する箇所の表示	関連する 請求の範囲の番号
A JP, 57-41028, A (石井泰) 6. (06.03.82)第1, 4, 7, 8図及び	3月 1982 その説明(ファミリーなし)	1 - 9
A JP, 63-2419, A (富士通株式会 (07.01.88)第1, 2図及びその説 JP, 3-181238, A (株式会社) (07.08.91)(ファミリーなし)	明 (ファミリーなし)	1 - 9
X C欄の続きにも文献が列挙されている。	□ パテントファミリーに関する別	川紙を参照。
* 引用文献のカテゴリー 「A」特に関連のある文献ではなく、一般的技術水準を示すもの 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献(理由を付す) 「O」口頭による開示、使用、展示等に言及する文献「P」国際出願日前で、かつ優先権の主張の基礎となる出願	て出願と矛盾するものではなく 論の理解のために引用するもの 「X」特に関連のある文献であって、 の新規性又は進歩性がないと考 「Y」特に関連のある文献であって、 上の文献との、当業者にとって よって進歩性がないと考えられ	、発明の原理又は理 当該文献のみで発明 えられるもの 当該文献と他の1以 自明である組合せに
国際調査を完了した日 06.06.00	国際調査報告の発送日 27.0	6 .00
国際調査機関の名称及びあて先 日本国特許庁(ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官(権限のある職員) 有泉良三 電話番号 03-3581-1101	* ************************************

国際調査報告

国際出願番号 PCT/JP00/01427

C(続き).	関連すると認められる文献	関連する
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	請求の範囲の番号
A	JP, 4-5773, A (株式会社 トキメック) 9. 1月 1992 (09.01.92)(ファミリーなし)	1 - 9